Special Issue

AI Security and Safety

Message from the Guest Editor

In this Special Issue, we aim to bring together researchers from the fields of adversarial machine learning, model robustness, model privacy, and explainable AI to discuss recent research and future directions for AI security, in particular, computer vision and pattern recognition. We invite submissions on any aspect of the security in deep learning systems (particularly computer vision and pattern recognition). We welcome research contributions related to, but not limited to, the following topics:

- Adversarial attacks and defenses for deep learning systems;
- Backdoor attacks and mitigations for deep learning models;
- Model stealing for AI applications and systems;
- Understanding the uncertainty and vulnerabilities of DNNs;
- Deepfake techniques on images and videos;
- Robustness of compact models and systems;
- Privacy-preserved deep learning;
- Explainable AI.

Guest Editor

Prof. Dr. Xianglong Liu
School of Computer Science and Engineering, Beihang University, Beijing 100191, China

Deadline for manuscript submissions

closed (15 March 2024)

Electronics

an Open Access Journal by MDPI

Impact Factor 2.6
CiteScore 6.1

mdpi.com/si/177768

Electronics
Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland
Tel: +41 61 683 77 34
electronics@mdpi.com

mdpi.com/journal/electronics

MDPI

Electronics

an Open Access Journal
by MDPI

Impact Factor 2.6
CiteScore 6.1

mdpi.com/journal/
electronics

MDPI

About the Journal

Message from the Editor-in-Chief

Electronics is a multidisciplinary journal designed to appeal to a diverse audience of research scientists, practitioners, and developers in academia and industry. The journal is devoted to fast publication of latest technological breakthroughs, cutting-edge developments, and timely reviews of current and emerging technologies related to the broad field of electronics. Experimental and theoretical results are published as regular peer-reviewed articles or as articles within Special Issues guest-edited by leading experts in selected topics of interest.

Editor-in-Chief

Prof. Dr. Flavio Canavero
Department of Electronics and Telecommunications, Politecnico di Torino, 10129 Torino, Italy

Author Benefits

High Visibility:

indexed within Scopus, SCIE (Web of Science), CAPlus / SciFinder, Inspec, Ei Compendex and other databases.

Journal Rank:

JCR - Q2 (Engineering, Electrical and Electronic) / CiteScore - Q1 (Electrical and Electronic Engineering)

Rapid Publication:

manuscripts are peer-reviewed and a first decision is provided to authors approximately 16.8 days after submission; acceptance to publication is undertaken in 2.4 days (median values for papers published in this journal in the first half of 2025).